OHIO AUDITOR OF STATE
KEITH FABER

# HB 96 – RC 9.64 Cybersecurity Requirements for Local Governments

**Torri Sholl,**
**Director of Policy & Legislative Affairs**
**Ohio Auditor of State**

OHIO AUDITOR OF STATE
**KEITH FABER**

## Mission of the Ohio Auditor of State

As Ohio's chief compliance officer, the Auditor of State makes Ohio government more efficient, effective, and transparent by placing checks and balances on state and local governments for taxpayers.

Efficient • Effective • Transparent

# Financial Statement Audit

- Currently, AOS audits for IT controls in financial audits.
- What IT controls do auditors look for currently?
  - IT Strategy – (IT planning and IT training)
  - Change Management (maintaining support, patches, upgrades)
  - Security Management (policies such as IT policies such as cyber policies and cyber awareness training programs)
  - System Level Access Controls (multi-factor, password controls, remote access, firewall)
  - Application Level Access Controls (multi-factor, role-based access, least privileged access)
  - Contracts with Vendors
  - Physical Security (contract, locked room, environmentally safe, access protection)
  - System Admin & Maintenance (vulnerability checks and monitoring up-time)
  - Backup (backups SHOULD BE TESTED and disconnected/offline)
  - Disaster recovery & business continuity (plan for what happens in a disaster, should have a copy off-site)

# AOS Bulletin 2024-003

- Ohio governments are increasingly falling victim to cybercrimes in the form of payment “re-direct” and business email compromise schemes.
- In 2023, the Auditor of State issued an Advisory alerting Ohio governments to an increase in cybercrime and providing guidance on what to look for and how to prevent attacks.
- This bulletin sets clear standards and expectations for Ohio governments and public employees regarding the handling of requests for payment re-directs.
- AOS has issued FFRs against fiscal officers for failing to follow protocols that resulted in the local government falling victim to cybercrimes.
  - Example: changing employee or vendor bank accounts to route payments to the bad actor's account.

# Payment Security Checklist (link on our website)

- Initial Review of Payment Information Change Request
  - Verify sender email address matches known contact. Look closely!
  - Hover over (don’t click) links to view and confirm legitimate URLs
  - Never open unsolicited attachments
  - Access websites directly instead of clicking links in the email.
- Verification Steps
  - FREEZE- No immediate action on any change request.
  - LOOK OUT FOR RED FLAGS from the requester.
  - REQUIRE any change in payment info be done in person.
  - SECONDARY VERIFICATION
  - DOCUMENT all verification attempts.
- Payment Processing
  - Separate staff handles payment initiation vs. approval.
  - Compare new payment details against historical records.
  - Flag any unusual payment amounts or destinations.
  - Require management approval for changes to: Banking information, contact details, payment instructions.

**Bulletin 2025-007:**

- Released 8/27/2025
- Compliance procedures will be developed and incorporated into the Ohio Compliance Supplement

## HB 96- RC 9.64 Background:

- The new requirements as passed in HB 96
  - Signed by Governor DeWine on June 30,2025
- Takes effect September 30, 2025
- Language can be found in ORC Section 9.64

## HB 96: Who does it apply to?

- Applies to all political subdivisions:
  - "Political subdivision" means a county, township, municipal corporation, or other body corporate and politic responsible for governmental activities in a geographic area smaller than that of the state.

- Compliance timeline for adoption of cyber program:
  - Counties and cities shall have a program adopted by **January 1, 2026**
  - For all other political subdivisions, the deadline will be **July 1, 2026**

- Compliance timeline for reporting incidents and approval of ransomware payments:
  - **September 30, 2025**

## HB 96 – RC 9.64: Overview

- Political subdivisions must:
  - Implement a cybersecurity program
  - Report cyber incidents to DPS and AOS
  - Obtain approval from their legislative body for ransomware payments

- This presentation is for information purposes only
  - Not legal advice
  - Political subdivisions should consult with their legal counsel and technology vendors to ensure compliance
  - DPS will be releasing additional guidance and instructions on compliance before the effective date.
  - AOS Bulletin 2025-007

## Cyber Program:

- The legislative authority of a political subdivision shall adopt a cybersecurity program that safeguards the entity’s data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.

- The program shall be consistent with generally accepted best practices for cybersecurity, such as, National Institute of Standards and Technology (NIST) cybersecurity framework and Center for Internet Security (CIS) cybersecurity best practices.

# Program Components:

- The program **MAY** include, but is not limited to the following:
    - Identify critical functions and risks
    - Assess the potential impact of breaches
    - Implement threat detection mechanisms
    - Establish incident response procedures
    - Plan for recovery and continuity
    - Define employee training requirements
        - Training from Ohio Persistent Cyber Initiation (O-PCI) could satisfy this requirement.
        - The O-PCI program delivered by the Ohio Cyber Range Institute (https://www.ohiocyberrangeinstitute.org/opci) and the Ohio Cyber Reserve (https://homelandsecurity.ohio.gov/ohio-cyber-integration-center/overview) includes online, hybrid and in person modules tailored to various types of organizations, from small to large, rural to urban and is funded by the State and Local Cybersecurity Grant Program.

## Ransomware Payment Restrictions-RC 9.64 (B)

- "A political subdivision experiencing a ransomware incident ***shall not*** pay or otherwise comply with a ransom demand unless the political subdivision's ***legislative authority formally approves*** the payment or compliance with the ransom demand in a r***esolution or ordinance*** that specifically states why the payment or compliance with the ransom demand is in the best interest of the political subdivision."

## Ransomware Payment Restrictions-

- If the legislative authority of a political subdivision make the decision pay or otherwise comply, they must adopt a resolution/ordinance in the public interest
- Section 121.22 (F)– Emergency meeting can be called with less than 24 hours notice and still be in compliance with Open Meetings

# Definition of Cybersecurity Incidents-RC 9.64(A)(1)

- A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
- Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by:
  - A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
  - A supply chain compromise.

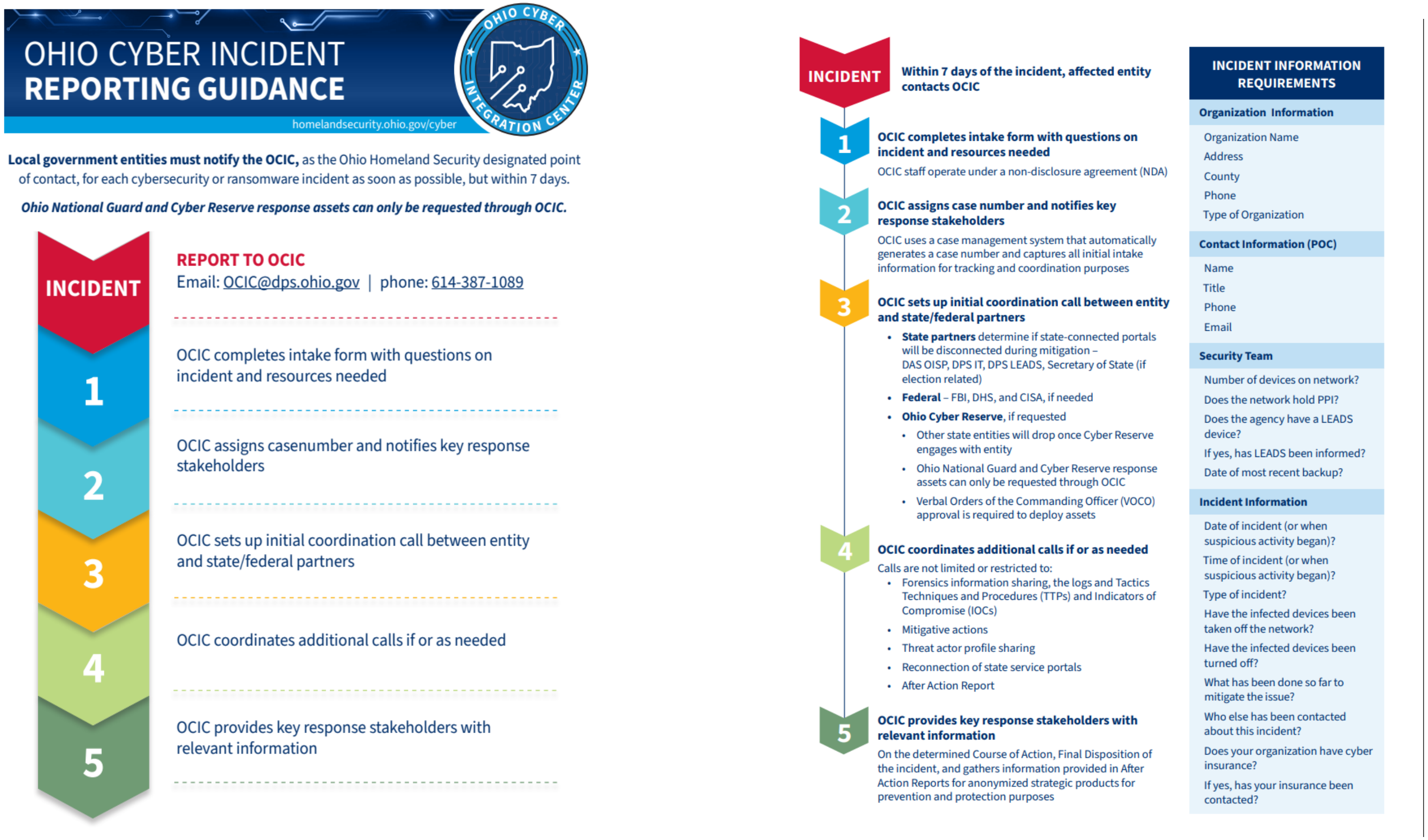
"Cybersecurity incident" does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial government entity.

## Cyber Incident Reporting Requirements – RC 9.64(D)

- After a Cyber or Ransomware Incident, Local Governments Must Notify both as soon as possible, but no later than:
  - Ohio Department of Public Safety
    - Within 7 days
    - To be submitted to the Ohio Cyber Integration Center (OCIC)
  - Ohio Auditor of State
    - Within 30 days

# Incident Reporting to OCIC:

- Report as soon as possible, but no later than seven days from discovery of incident
- Provide organization details and incident specifics:
  - Name, address, county, phone, organization type
  - POC: name, title, phone, email
  - Date/time of incident or suspicious activity
  - Type of incident, mitigation steps taken prior to reporting
  - Affected devices removed/turned off?
  - Cyber insurance status & provider contacted?
  - Others contacted regarding the incident?
  - Security team details: device count, PPI presence, state connected device, last backup date



# OHIO CYBER INCIDENT REPORTING GUIDANCE

homelandsecurity.ohio.gov/cyber

**Local government entities must notify the OCIC,** as the Ohio Homeland Security designated point of contact, for each cybersecurity or ransomware incident as soon as possible, but within 7 days.

***Ohio National Guard and Cyber Reserve response assets can only be requested through OCIC.***

**INCIDENT**

**REPORT TO OCIC**
Email: OCIC@dps.ohio.gov | phone: 614-387-1089

**1** OCIC completes intake form with questions on incident and resources needed

**2** OCIC assigns casenumber and notifies key response stakeholders

**3** OCIC sets up initial coordination call between entity and state/federal partners

**4** OCIC coordinates additional calls if or as needed

**5** OCIC provides key response stakeholders with relevant information

**INCIDENT** **Within 7 days of the incident, affected entity contacts OCIC**

**1** **OCIC completes intake form with questions on incident and resources needed**

OCIC staff operate under a non-disclosure agreement (NDA)

**2** **OCIC assigns case number and notifies key response stakeholders**

OCIC uses a case management system that automatically generates a case number and captures all initial intake information for tracking and coordination purposes

**3** **OCIC sets up initial coordination call between entity and state/federal partners**

- **State partners** determine if state-connected portals will be disconnected during mitigation – DAS OISP, DPS IT, DPS LEADS, Secretary of State (if election related)
- **Federal** – FBI, DHS, and CISA, if needed
- **Ohio Cyber Reserve**, if requested
  - Other state entities will drop once Cyber Reserve engages with entity
  - Ohio National Guard and Cyber Reserve response assets can only be requested through OCIC
  - Verbal Orders of the Commanding Officer (VOCO) approval is required to deploy assets

**4** **OCIC coordinates additional calls if or as needed**

Calls are not limited or restricted to:

- Forensics information sharing, the logs and Tactics Techniques and Procedures (TTPs) and Indicators of Compromise (IOCs)
- Mitigative actions
- Threat actor profile sharing
- Reconnection of state service portals
- After Action Report

**5** **OCIC provides key response stakeholders with relevant information**

On the determined Course of Action, Final Disposition of the incident, and gathers information provided in After Action Reports for anonymized strategic products for prevention and protection purposes

## INCIDENT INFORMATION REQUIREMENTS

**Organization Information**

Organization Name
Address
County
Phone
Type of Organization

**Contact Information (POC)**

Name
Title
Phone
Email

**Security Team**

Number of devices on network?
Does the network hold PPI?
Does the agency have a LEADS device?
If yes, has LEADS been informed?
Date of most recent backup?

**Incident Information**

Date of incident (or when suspicious activity began)?
Time of incident (or when suspicious activity began)?
Type of incident?
Have the infected devices been taken off the network?
Have the infected devices been turned off?
What has been done so far to mitigate the issue?
Who else has been contacted about this incident?
Does your organization have cyber insurance?
If yes, has your insurance been contacted?

# Incident Reporting to AOS:

- Report as soon as possible, but no later than 30 days upon discovery of an incident
- Questions on AOS Report Form include:
  - POC: name, title, email, phone
  - Government entity type
  - Date/time of incident and type of incident
  - Was any data compromised?
  - Was there a loss of funds? If yes, how much?
  - Was ransom demanded? If so, was it paid?
  - If ransom was paid, what is the ordinance or resolution approving payment?
  - Were policies and procedures in place at the time of the event?

## Contact Info to Report:

- Ohio Cyber Integration Center
  - Phone: 614-387-1089
  - Email: OCIC@dps.ohio.gov
  - Website: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center
- Ohio Auditor of State
  - Phone: 866-FRAUD-OH
  - Reporting Form: ohioauditor.gov/fraud/docs/CybersecurityReportingForm.pdf
  - Email: cyber@ohioauditor.gov
  - Website: www.ohioauditor.gov

## Public Records Exemption – RC 9.64(E):

- To protect information form bad actors, records related to:
  - Cybersecurity programs
  - Incident reports and procurement documents are not public record under ORC 149.43

## Key Takeaways:

- All local governments must implement cyber programs
  - Counties and cities by January 1, 2026
  - All other political subdivisions by July 1, 2026
- Ransom payments require formal approval by the legislative authority
- Cyber incidents must be reported within specific timeframes
  - DPS within 7 days
  - AOS within 30 days
- AOS Compliance procedures will be developed and incorporated into the Ohio Compliance Supplement

# Resources Available:

CyberOhio & State of Ohio Capabilities to Support Compliance
The following state-led programs are available to assist local governments in meeting some of the cybersecurity requirements of HB 96

- Ohio Cyber Reserve
- Ohio Cyber Range
- Ohio-Persistent Cyber Initiative
- Each offers a defined pathway for risk assessment, training, incident response planning, and long-term cyber maturity.
- CyberOhio will provide for future deeper dive webinars on each capability

## CYBERSECURITY TRAINING

**Annual Training**

- Tailored to job duties
- May be provided by the State of Ohio
- LGEs are encouraged to utilize existing capabilities provided by their MSPs.
- Free training offered by:
  - **Ohio Persistent Cyber Initiative (O-PCI)**
  - **Ohio Cyber Reserve**

## O-PCI

**Free Cybersecurity Training for Local Government Entities**

- Whole-of-organization training
- Tailored to the roles of employees (Executive/IT/General)
- Includes online modules, creation of plans/policies/procedures, cyber exercises, and vulnerability assessments

**OHIO PERSISTENT CYBER IMPROVEMENT**

**ohiocyberrangeinstitute.org/opci**

*9,000+ public employees have completed 8,000+ hours of training in counties, cities, libraries, schools, and health districts across Ohio.*

*BONUS Resource: Cyber Frontline First Aid Kit (CFFAK)*
**ohiocyberrangeinstitute.org/cffak**

## Questions?

- Refer to Bulletin 2025-007
- Email us at Cyber@ohioauditor.gov
- Call us at 866-FRAUD-OH

- For Cybersecurity related questions, please reach out to CyberOhio at Cyber.ohio.gov